UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,020	07/21/2000	Alexandre F. Tenca	245-53434	4090

7590 08/17/2004

Klarquist Sparkman Campbell Leigh & Whinston LLP
One World Trade Center
Suite 1600
121 SW Salmon Street
Portland, OR 97204

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,020	TENCA ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted on January 18, 2002 and December 7, 2001 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-3,5-8,11-13,15, and 16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims currently recite of software alone and of itself and do not fall into a statutory class. It is suggested by the examiner that the claims be amended to include a computer readable medium containing instructions for performing Montgomery multiplication/product as is recited in the respective dependent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-3,5-8,11-13, and 15-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Monier et al. The examiner notes that the applicant's claim language is bracketed next to the prior art's similar limitations.

As per claim 1, Monier et al discloses of a method for performing Montgomery multiplication by disclosing of receiving a multiplicand (first operand) and a multiplier (second operand)(col. 3, lines 38-42). The multiplicand (first operand) is represented as m words (at least two words)(col. 3, lines 38-45 and col. 4, lines 12-16). The multiplier (second operand) is represented as a series of k bits (col. 3, lines 38-45 and col. 4, lines 12-16). The Montgomery product of the multiplicand (first operand) and the multiplier (second operand) is performed by multiplying the words representing the multiplicand (first operand) by the bits representing the multiplier (second operand)(col. 3, lines 38-50 and col. 4, lines 12-16).

As per claim 2, Monier et al of discloses of a method for performing Montgomery multiplication (product) wherein a multiplicand (first operand X) and a multiplier (second operand Y) with respect to Modulus N (M)(col. 3, lines 38-42) is received. The multiplicand (first operand X) and multiplier (second operand Y) are represented as m words and as a series of k bits (col. 3, lines 38-45 and col. 4, lines 12-16).

As per claim 3, Monier et al teaches of a predetermined (previously selected) number of words representing the multiplicand (first operand) and the modulus (col. 3, lines 39-54).

As per claim 5, Monier et al discloses of a method for performing Montgomery multiplication (product) by disclosing of receiving a multiplicand (first operand X) and a multiplier (second operand Y) with respect to Modulus N (M)(col. 3, lines 38-42). The multiplicand (first operand X) and multiplier (second operand Y) are represented as m words and as a series of k bits (col. 3, lines 38-45 and col. 4, lines 12-16). A word length of k bits and a number of words p (e) is selected (col. 3, lines 38-54). The multiplier (second operand Y) and Modulus N (M) are represented as p (e) words) of length k (w) bits (col. 3, lines 38-54 and col. 4, lines 12-16) wherein it is interpreted by the examiner that p (e) words can be any value, including at least 2. An intermediate value of a first word of the Montgomery multiplication (product) is obtained based on the product of a word of the multiplier (second operand) and a bit of the multiplicand (first operand)(col. 3, lines 38-54 and col. 4, lines 1-28).

As per claim 6, it is taught by Monier et al that product of the word length k (w) bits and the number of words p (e) is we $\geq$ m (col. 3, lines 39-54 and col. 16, lines 5-12).

As per claim 7, Monier et al recites of obtaining an intermediate value of a second word of the Montgomery product based on a product of a second word of the multiplier (second operand) and a second bit of the multiplicand (first operand) in parallel with obtaining the intermediate value of the first word (col. col. 3, lines 39-54 and col. 4, lines 4-28).

As per claim 8, it is disclosed by Monier et al of updating the intermediate value of the first word of the Montgomery product with a contribution from at least one product of a second selected bit of the multiplicand (first operand) with at least a second selected word of the multiplier (second operand)(col. 3, lines 39-54 and col. 4, lines 4-28).

As per claim 11, Monier et al teaches of a method for coding plaintext, the plaintext is represented as a series of binary bits and performing word-wise by bit-wise Montgomery multiplication of a digital representation of the plaintext with a multiplier (col. 3, lines 38-45 and col. 5, lines 57-63).

As per claim 12, it is disclosed by Monier et al that the multiplier is the digital representation of the plaintext (col. 5, lines 57-63).

As per claim 13, Monier et al teaches of a method for decrypting (decoding) a ciphertext, wherein word-wise by bit-wiser Montgomery multiplication of a digital representation of the ciphertext with a multiplier is performed (col. 3, lines 38-45, col. 5, lines 57-63, and col. 12, lines 45-50).

As per claim 15, Monier et al recites of a method for supplying a multiplicand (first operand) and a multiplier (second operand) to a Montgomery multiplication circuit (module)(col. 3, lines 38-50). A word length of k (w) bits and a number of words p (e) is selected (col. 3, lines 38-54). The multiplier (second operand) is represented as p (e) words of length w (col. 3, lines 38-45 and col. 4, lines 12-16). The words of the multiplier (second operand) are delivered to the Montgomery multiplication circuit (module)(col. 3, lines 38-45 and col. 4, lines 12-45).

As per claim 16, it is taught by Monier et al of representing a modulus N (M) as p(e) words of length k (w) bits (col. 3, lines 38-45 and col. 4, lines 12-16). The words of the modulus are delivered to the Montgomery multiplication circuit (module)(col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 17, the teachings of Monier et al disclose of a circuit (apparatus) for performing Montgomery multiplication of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words of the multiplicand (first operand), words of the modulus, an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45). A control unit is also shown in Figure 1 that is situated and configured to direct words of the multiplicand (first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 18, Figure 1 of Monier et al also demonstrates of a data path along which words of the multiplicand (first operand) and multiplier (second operand) are delivered to the processing elements (col. col. 3, lines 38-49).

As per claim 19, Figure 1 of Monier shows of processing elements, it is implied that task processors are contained within the teachings since task processors are dedicated towards specific responsibilities and in light of the teachings of Monier et al, to perform Montgomery multiplication. These devices receive words of the multiplicand

(first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 20, the teachings of Monier et al disclose of a circuit for performing Montgomery multiplication (product) of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words of the multiplicand (first operand), words of the modulus, an output that delivers values of words of the Montgomery multiplication (product)(col. 3, lines 38-45 and col. 4, lines 12-45). Monier et al also demonstrates in Figure 1 of a data path along which words of the multiplicand (first operand) and multiplier (second operand) are delivered to the processing elements (col. col. 3, lines 38-49).

As per claim 21, Monier et al recites of inputs for receiving words of the multiplicand (first operand), an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45).

As per claim 22, Figure 1 demonstrates of a data path configured to provide a first selected bit of the multiplier (second operand) to the first processing element and a second selected bit of the multiplier (second operand) to a second processing element (col. 3, lines 38-45 and col. 4, lines 12-45).

As per claim 23, the teachings of Monier et al disclose of a circuit (apparatus) for performing Montgomery multiplication of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a

plurality of processing elements, it is implied that task processors are contained within the teachings since task processors are dedicated towards specific responsibilities and in light of the teachings of Monier et al, to perform Montgomery multiplication, that includes inputs for words of the multiplicand (first operand), words of the modulus, an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45). A computational unit is also shown in Figure 1 that determines a contribution to an intermediate value of a word of the Montgomery multiplication (product) based on the received bit of the multiplicand (first operand) and the received words of the multiplier (second operand) and the modulus and outputting the intermediate value of the word of the Montgomery multiplication (product)(col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 24, Figure 1 of Monier shows of processing elements, it is implied that task processors are contained within the teachings since task processors are dedicated towards specific responsibilities and in light of the teachings of Monier et al, to perform Montgomery multiplication. These devices receive words of the multiplicand (first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 25, the teachings of Monier et al disclose of a circuit (apparatus) for performing Montgomery multiplication of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words (messages) of the multiplicand (first operand), words of the modulus, an intermediate value of a word of

Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45). A control unit is also shown in Figure 1 that is situated and configured to direct words of the multiplicand (first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 26, the teachings of Monier et al disclose of a circuit (smart card) for performing Montgomery multiplication (product) of a multiplicand (first operand) and a multiplier (second operand)(col. 3, lines 38-49). Figure 1 shows a plurality of processing elements. The circuit (smart card) performs word-wise by bit-wise Montgomery multiplication (col. 3, lines 38-45).

As per claim 27, Monier et al discloses that the multiplicand (first operand) and the multiplier (second operand) are non-zero values (col. 3, lines 38-49) and it is interpreted by the examiner that these values can be equal.

As per claim 28, it is taught by Monier et al that the values, or first operand, can be an authentication value (col. 1, lines 7-15 and col. 3, lines 38-45).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4,9,10, and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Monier et al.

The teachings of Monier et al disclose of performing Montgomery multiplication by disclosing of receiving a multiplicand (first operand) and a multiplier (second operand)(col. 3, lines 38-42). The teachings of Monier et al are silent in disclosing of a computer readable medium containing instructions for performing the Montgomery multiplication. The examiner hereby takes official notice that the use of a computer readable medium containing instructions is notoriously well known. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply use of a instructions contained on a computer readable medium as a means of using a computer to execute a software program intended to use Montgomery multiplication. The examiner hereby asserts that it would have been obvious that the teachings comprise a computer readable medium for storing instructions and a processor coupled to memory that is configured to execute the computer readable code in order for the teachings to be performed as disclosed. The software program (computer readable code) and necessary hardware (processor and computer readable medium) to perform the necessary tasks are notoriously known to one of skill in the art

as an essential part of computing. It is obvious that the teachings exist in the form of a software program (computer readable code) and are utilized by the hardware, namely stored in memory and a processor interprets, processes, and performs the task of Montgomery multiplication.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Powell et al, U.S. Patent 6,282,290

McGregor, U.S. Patent 6,240,436

Koc et al, "A Reduction Method for Multiplication in Finite Fields"

Su et al, "An Improved Montgomery's Algorithm for High-Speed RSA Public-Key Cryptosystem

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

August 6, 2004

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100